



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/661,049	09/14/2000	Terence R. Spies	MS1 503US	8207
22801	7590	10/13/2005	EXAMINER	
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			NOBAHAR, ABDULHAKIM	
			ART UNIT	PAPER NUMBER
			2132	
DATE MAILED: 10/13/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/661,049

Applicant(s)

SPIES, TERENCE R.

Examiner

Abdulahakim Nobahar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 July 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7, 9, 10, 12-22, 24, 25, 27-32, 35-37, 39-49, 51-63, 65-77 and 79-81 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7, 9-10, 12-22, 24, 25, 27-32, 35-37, 39-49, 51-63, 65-77 and 79-81 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

Claim 72 is objected to because of the following informalities: This claim recites "a data block to be encrypted by an encryption key" as one of the comprised elements of a system, which is not a physical element. Also the last three elements of this claim do not appropriately define physical elements of a system. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 31, 32, 35-37 and 39-43 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim 31 in its preamble recites: "An arrangement comprising". If the "arrangement" is assumed to be an apparatus, then none of the elements of this claim describe the physical elements of an apparatus, because they are directed to performing logic instructions. Therefore, this is non-statutory.

Response to Arguments

1. Applicant's arguments filed July 25, 2005 have been fully considered but they are not persuasive.

2. With respect to independent claims 1, 16, 31, 44, 58 and 72, applicant argues that "The Hardy reference does not teach or suggest generating multiple random numbers, signing one of the random numbers, and creating an encryption key by hashing a combination of the signed random number and the other random number." see, for example, page 22. Applicant also argues that "Next, the Epstein reference also does not teach or suggest generating multiple random numbers, signing one of the random numbers, and creating an encryption key by hashing a combination of the signed random number and the other random number." see, for example, page 23.

Hardy discloses a system that combines a hashed document (corresponding to the recited digitally signing a first string) a generated value, k1 (corresponding to the recited second random value), preferably by concatenating them to produce an intermediate value, k2. Hardy further discloses that the system hashes the produced k2 to generate a key (a pseudo-random key) (see column 10, lines 20-35 and Fig.3). On the other hand, Epstein teaches a system that comprises a random number generator that generates random numbers (see column 2, lines 55-60). Epstein further discloses that the system provides (i.e., generates) a plurality of data items (i.e., random numbers) to a signing device (see column 2, line 66-column 3, line 11). The combined teachings of Hardy and Epstein would meet the limitations of claimed invention. Therefore, it is obvious that at the time of the invention, a person skilled in the art would be motivated to combine the teaching of Epstein in the system of Hardy to have a more secure system with a random generator capable of generating a multiple random numbers to compute a cryptographic key.

3. In light of the above submission the previous rejection of the claims is maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1-7, 9-10, 12-22, 24, 25, 27-32, 35-37, 39-49, 51-63, 65-77 and 79-81 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al. (6,079,018; hereinafter Hardy) in view of Epstein (6,453,416 B1).

2. Regarding claims 1, 2, 12, 16-17, 31-32, 58 and 72, Hardy discloses a method and a system for digitally signing a document by applying a predefined one-way hash function to the document (see, for example, abstract). Hardy discloses that a value, K1, (corresponding to the recited random value) is generated and this value is combined with a hash value of a document, H, which is generated by a hashing procedure (corresponding to the recited digitally signing a first or a second data string) in order to produce an intermediate value, K2, (see, for example, col. 8, lines 8-22; col. 10, lines 20-49; Fig. 3). Hardy further discloses that the intermediate value is hashed to generate a pseudo-random key, K, (corresponding to the recited generating an encryption key). Then the key is used to produce a digital signature of the document,

Art Unit: 2132

which is a string of bit value (corresponding to the recited encrypting the data block) (col. 2, lines 25-32). The Hardy's system only generates one value as an input for generating an encryption key. Although it uses a document as a second value, but it does not expressly disclose generation of a second random value.

Epstein, however, teaches a secure signing device and a method for using such a device to create a digital signature (corresponding to the recited encrypting the data block) (col. 1, lines 13-16; col. 2, lines 29-39). Epstein further teaches that a number of data strings are provided by a computer system (corresponding to the recited generated or accessed by a first device) (abstract and col. 2, lines 66-67) and hash of one of the data is computed (col. 2, lines 40-53).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the generation of a number of data items as taught in Epstein in the system of Hardy to be used in calculation of a hash value and generation of an encryption key, because it would provide for preventing the possibility that an imposter utilizes the signing device (i.e., smart card) (col. 2, lines 30-39).

3. Regarding claims 3 and 18, Hardy discloses that a random value, K, is generated and it is combined with a hash of a document (corresponding to the recited the third random value) in order to encrypt the combination using a private key, x, to generate a digital signature (see Fig. 1).

4. Regarding claims 4 and 19, these claims are rejected as applied to the like elements of claim 3 and further the following:

Epstein discloses a verification process that decrypts a digital signature of a document (corresponding to the recited data block) using a decryption key to obtain the hash value of the document (see col. 1, lines 17-34; col. 5, line 63-col. 6, line 27).

Epstein further discloses that a second hash value of the document using a secure hash function is derived. The second hash value is compared with the first hash value obtained from the decryption operation to verify the authenticity of the document.

5. Regarding claims 5, 7, 20, 22 and 35-37, Hardy discloses a non-volatile memory in a computer system that stores durably data including private key, other secret information and a hash value of a document (i.e., a data string) (see, for example, col. 9, lines 6-20; col. 9, lines 60-65; col. 13, lines 41-45; Fig. 2).

6. Regarding claims 6 and 21, these claims are rejected as applied to the like element of claim 1 as stated above.

7. Regarding claims 9-10, 22, 24-25, and 39-40, Hardy discloses that a pseudo-random key is generated by cryptographically hashing combination (i.e., concatenation) of a document digest (corresponding to the recited the digitally signed first string) with another value (corresponding to the recited the third data string) (see, for example, Fig. 3, 142A; col. 8, lines 8-13).

8. Regarding claims 13-15, 28-30, and 43, Hardy discloses that a smart card as a portable device is suitable to be used for digitally signing a value in order to generate a signature (col. 7, lines 27-47).

9. Regarding claims 27, 42, 44, 54 and 68, these claims are rejected as applied to the like elements of claims 1, 5 and 16 as stated above.

10. Regarding claims 13-15, 28-30, 43, 55-57 and 69-71, Epstein discloses a signing device such as a smart card that digitally signs a value and generate a signature, for example, of a document to be authenticated (col. 2, lines 30-54).

11. Regarding claim 41, Hardy discloses a mechanism for selecting randomly a seed value for the computation of encryption key (see, for example, col. 6, lines 6-13).

12. Regarding claims 45-47, 59-61 and 73-75, these claims are rejected as applied to the like elements of claims 4-6 as stated above.

13. Regarding claims 46-47, 59-61 and 74, Epstein discloses that after receiving (corresponding to the recited accessing) data, the data is decrypted using an encryption key (see, for example, col. 6, lines 12-20) and the result of the decryption is a hash value.

14. Regarding claims 48, 49, 62, 63, 76 and 77, Epstein discloses a memory system that the provided data strings are read from (see, for example Fig. 1, block 146).

15. Regarding claims 51-52, 65-66 and 79-80, Hardy discloses that a pseudo-random key is generated by cryptographically hashing combination (i.e., concatenation) of a document digest (corresponding to the recited the digitally signed second data) with another value (corresponding to the recited the third data string) (see, for example, col. 8, lines 8-13).

16. Regarding claims 53, 67 and 81, Hardy discloses a mechanism for selecting randomly a seed value for the computation of encryption key (see, for example, col. 6, lines 6-13).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulahakim Nobahar
Examiner
Art Unit 2132 *A.N.*

October 6, 2005

Gilberto Barron Jr.
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100